

IT Security Handbook

Managed Elevated Privileges (EP) Implementation Guidance Handbook

ITS-HBK-0004A

Effective Date: 20100415

Expiration Date: 20110415

Responsible Office: OCIO/Deputy CIO for Information Technology Security

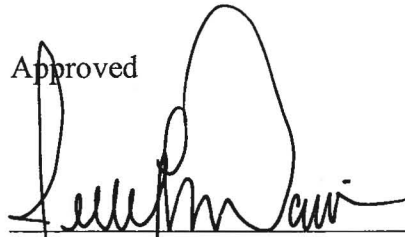
Contents

Change History	iii
1. Introduction and Background	1
2. Rationale for Managing Elevated User Privileges	1
2.1 Why is NASA Limiting Elevated Privileges?	1
2.2 Why is NASA Managing Elevated Privileges?	2
2.3 Does FDCC mandate limiting EP?	2
3. Scope of the Policy and Procedures	3
3.1 On what systems do EP have to be managed?	3
3.2 On what devices do EP have to be managed?	3
3.3 Do the requirements apply to elevated user privileges in applications?	3
3.4 To whom do the requirements apply?	3
3.5 What level(s) of privileges do the requirements apply to?	3
3.6 When do elevated user privileges need to be requested?	4
3.7 What kind of request for EP is reasonable?	4
3.8 What is the deadline for compliance with the policy?	4
4. Requesting and Approving Elevated User Privileges	5
4.1 Which NAMS workflow should be used for managing EP on a system?	5
4.2 Do I need to create an EP NAMS workflow for my system?	6
4.3 How do I create an EP NAMS workflow for my system?	6
4.4 How do I use the default EP NAMS workflow as a requester?	6
4.5 How do I use the default EP NAMS workflow as a system owner?	9
4.6 How do I use the default EP NAMS workflow as an approver?	10
4.8 Additional questions	10
5. Training	11
5.1 What training is needed for whom/what kind of request?	11
5.2 When should a user take the training?	12
5.3 Who determines what training is acceptable and how?	12
5.4 Who verifies that qualification requirements have been met?	12
5.5 Why are qualification requirements based on the length of the request instead of the level of privileges requested?	13
6. Waivers	13
6.1 What kinds of waivers are possible and who can approve them?	13
6.2 How do I get a waiver?	14
6.3 How should waivers be tracked?	14
6.7 Can waivers be renewed?	14
7. Miscellaneous	14
7.1 How will EP be managed on an ODIN device?	14
Appendix A. Acronyms	15
Appendix B. Definitions	16
Appendix C. References	19
Appendix D: Memorandum Delegating Waiver Authority and Responsibility for Selected Requirements for Managing Elevated User Privileges on NASA IT Devices.	20

Distribution:

NODIS

Approved

A handwritten signature in black ink, appearing to read "Jerry L. Davis", written over a horizontal line.

Jerry L. Davis
Deputy Chief Information Officer for
Information Technology Security

4/20/10

Date

Change History

ITS-HBK-0004A Managed Elevated Privileges (EP) Implementation Guidance Handbook

Change Number	Date	Change Description
1	04/15/2010	Table 5.1.2 updated with current training information

1. Introduction and Background

- 1.1 This document provides guidance on implementing NASA policy on managing elevated user privileges (EP) on NASA IT devices, as stated in NASA Interim Technical Requirements (NITR) 2810-14A.
- 1.2 NASA decided to manage elevated user privileges on July 26, 2006, based on the NASA Deputy Administrator's memo, "Meeting NASA Information Technology Security Requirements." In May, 2008, the NASA IT Management Board set out more detailed requirements on managing elevated user privileges, for example, that Center CIOs were to be the approval authority for elevated privileges, that elevated privileges could be held for no more than 12 months without re-approval, and that NAMS should be used to manage elevated privilege requests.
- 1.3 The majority of this document is in the form of frequently asked questions, with answers, organized in the following sections: (2) rationale for managing elevated user privileges, (3) scope of the policy and procedures, (4) requesting and approving elevated user privileges, (5) training, (6) waivers, and (7) miscellaneous. The appendices include a list of common acronyms, definitions of terms, and references.
- 1.4 The guidance in this document applies to all NASA information systems and NASA employees and contractors.
- 1.5 Agency-wide implementation of the requirements for managing elevated user privileges is not complete and several implementation issues remain to be addressed. It is anticipated that this documented will be updated as additional details and guidance become available.

2. Rationale for Managing Elevated User Privileges

2.1 Why is NASA Limiting Elevated Privileges?

NASA is limiting elevated users privileges on all IT devices to reduce the risks to these devices, to NASA information, and to the computing environment; to adhere to industry best practices; and to comply with Federal regulations, policy and guidance.

Accessing information systems with elevated user privileges greatly increases the risks of security incidents and of unintended and/or detrimental changes to system configurations. For example, most viruses, trojans, and spyware install and run under the rights and privileges of the currently logged on user. When a user accesses a computer with elevated user privileges, any malicious software that finds its way on to the computer will initially install and run with elevated privileges, increasing the potential damage. In addition, a user accessing a computer with elevated privileges has a much greater ability to inadvertently or maliciously change the configuration of the IT device, potentially creating security risks for the IT device and its environment, bringing the IT device out of compliance with NASA standard configurations, or rendering the IT device unusable.

It is considered best practice to restrict user rights in order to limit the scope and lessen the opportunity of attacks. One analysis found that 92% of the vulnerabilities patched by Microsoft in 2008 could have been eliminated or made less dangerous by having users run Windows as regular users and not have administrative rights.

[http://www.cio.com/article/479228/Removing_Admin_Rights_Stymies_of_Microsoft_s_Security_Vulnerabilities]

Federal regulations and guidance, as well as NASA policy, require that only persons with a need for elevated privileges on IT systems have that level of access. This is expressed in multiple policy statements, most notably in a 2006 memorandum from Shana Dale (see NASA Memo “Meeting NASA Information Technology Security Requirements”, July 26, 2006). NIST and OMB have made statements about avoiding the general use of elevated system privileges, NIST in its FDCC FAQ, and OMB in a memorandum regarding Federal Agency procurements and FDCC (OMB Memorandum M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*, June 1, 2007). Several security controls in NIST SP 800-53 Rev 3, also spell out these requirements (AC-2 control enhancement 7, AC-6 control enhancement 3).

However, NASA has to ensure that security measures, such as limiting elevated user privileges, do not interfere with the Agency’s mission and operations. Therefore, if a NASA employee needs elevated user privileges on a device to perform their duties, these privileges should be granted, provided that the employee understands the risks and responsibilities associated with elevated privileges and the employee uses the elevated privileges appropriately and for the purposes for which they were granted.

2.2 Why is NASA Managing Elevated Privileges?

NASA is managing elevated user privileges on all IT devices in order to

- Limit elevated privileges as much as possible: Managing EP allows the Agency to make sure that only those employees that need these privileges will have them and to ensure that anyone who holds EP is qualified (i.e. understands the risks and responsibilities).
- Understand where, why, and by whom elevated privileges are needed: Such an understanding may allow NASA to improve application development (i.e. develop applications in ways to limit the need for elevated privileges to run them) and to modify existing applications, processes, and contracts to reduce the need for elevated user privileges.
- Maintain a record of who has elevated privileges on which devices: This information is useful for incident response and analysis and vital to ensure user accountability.
- Ensure controlled management of the IT environment: Effective formal processes for granting and monitoring elevated user privileges will facilitate any changes to the IT environment (e.g. Agency-wide deployment of a new operating system, transition to new service providers, etc.).

2.3 Does FDCC mandate limiting EP?

There are no FDCC settings or measurement controls designed to check for elevated privileges. There is currently no requirement enforced by the settings found in the FDCC XCCDF that disallows the membership of user accounts in the Administrators, Power User, or other group

with elevated privileges on Windows systems, as a condition of FDCC compliance. Properly managed, elevated privileges can be granted to all who require them.

Office of Management and Budget FDCC policy mandates (OMB memo M-07-18), while not part of the FDCC settings or checks themselves, recommend that Federal Agencies insert contract language stating that vendors must certify that: "c) Applications designed for normal end users shall run in the standard user context without elevated system privileges." The design of Federal IT systems and service delivery must take this into account, regardless whether or not XCCDF checks exist to affect FDCC system compliance scoring in the presence of elevated end user privileges.

3. Scope of the Policy and Procedures

3.1 On what systems do EP have to be managed?

The requirements in NITR 2810-14 apply to all NASA information systems, i.e. those systems that have a NASA system security plan (SSP). They do not apply to external, or contractor, systems.

3.2 On what devices do EP have to be managed?

The requirements in NITR 2810-14 apply to all IT devices that have multiple privilege level capabilities. This includes desktops, laptops, workstations, servers, routers, printers and any other devices that can enforce user access control at multiple privilege levels. It also includes OAIT, non-OAIT and special purpose devices with these capabilities.

3.3 Do the requirements apply to elevated user privileges in applications?

The requirements in NITR 2810-14 apply only to elevated user privileges at the operating system (OS) level. Elevated privileges at the application level are not within the scope of NITR 2810-14.

3.4 To whom do the requirements apply?

The requirements in NITR 2810-14 apply to all NASA employees, contractors and others who access NASA systems and NASA IT devices. This includes guests, regular users, system administrators and any other users.

3.5 What level(s) of privileges do the requirements apply to?

Elevated privileges are any access rights or permissions that allow the user that holds them to access system control, monitoring, or administration functions. This includes functions such as installing, upgrading, significantly changing or patching software, including the computer's operating system.

The requirements in NITR 2810-14A apply to any and all privileges above basic user privileges, except as noted in this section.

The requirements in NITR 2810-14A do not apply to

- Membership in the “network configuration operators” group, which allows a user to change the IP address of the device. This set of rights does not require a NAMS request because it is considered to pose minimal risk.
- Membership in the “remote desktop users group”, which allows a user to establish a remote session on the device from another device. This set of rights does not require a NAMS request because it only affects the user’s ability to remotely connect to the device and does not increase the user’s level of privilege.

3.6 When do elevated user privileges need to be requested?

An EP request must be completed and approved before elevated privileges can be granted on a NASA IT device.

Users that held EP before the NASA policy was issued must have a documented approved request for these privileges in NAMS within 6 months of the issuance of NITR 2810-14A in order to retain their elevated privileges.

If elevated privileges are still needed at the expiration of a NAMS EP request, renewals (i.e. follow-on requests) should be entered into NAMS in time to allow review and approval of the request before the original request expires. Depending on qualification requirements being met and on the availability of the sponsor and approver, this should be expected to take at least 1-3 business days.

3.7 What kind of request for EP is reasonable?

The relevant Center CIO, as the approver, determines whether a particular request for EP is reasonable. This determination should be made based on the justification documented in the NAMS request, the security categorization of the system, and other circumstances. Some examples of justifications that might be approved include:

- An application that the user runs in performing their his/her duties (finance, payroll, HR specific applications or tools) requires elevated privileges on the computer’s operating system in order to run.
- The person requesting the elevated privileges is a system administrator.

3.8 What is the deadline for compliance with the policy?

Any new elevated user privileges for existing users must be requested and approved in accordance with the policy.

Any existing elevated privileges must be documented within NAMS within 6 months of the effective date, i.e. by February 17, 2010.

After December 17, 2009, all new user accounts and account renewals must, by default, be issued with only the user-level privileges. If the user needs EP, they must be requested and approved in NAMS in accordance with the policy (NITR 2810-14A).

4. Requesting and Approving Elevated User Privileges

4.1 Which NAMS workflow should be used for managing EP on a system?

OCIO has identified two different use cases for managing EP in NAMS.

1. **Elevated privileges for system administrators on devices that are managed through NCAD** are already being managed throughout the Agency using the AD Resource Management Account workflow or “AA” Account in NAMS (AGCY0025 NCAD Resource Admin).
2. **All other elevated privileges**, including for users on NCAD-managed devices and for everyone on any device not managed through NCAD, may be managed through one of the following.

- a. Using the default EP NAMS workflow (AGCY0027 ElevPriv_Agency).

OR

- b. Using a NAMS workflow determined by the system owner or Center (see below).

All elevated privileges on ODIN-managed devices will be requested either through workflow AGCY0025 (use case 1) or through workflow AGCY0027 (use case 2.a).

If a Center or system owner chooses to develop a new NAMS workflow or to use an existing workflow other than the above for managing EP on a system (i.e. use case 2.b), the following requirements apply:

1. The workflow must meet the requirements for EP workflows as indicated in section 1.8 of NITR 2810-14A “Managed Elevated Privileges on NASA IT Devices.
2. The Center or system owner is responsible for informing the users of which workflow they should use to request elevated privileges on the devices/system in question.
3. The SSP must reference the new/different NAMS workflow(s) which are being used to manage elevated privileges.
4. All new/different NAMS workflows must be reported to the NASA OCIO, at itsactions@mail.nasa.gov, along with the SSP and/or device(s) for which they are being used to manage EP. This is to ensure that there is a registry of all NAMS workflows being used to manage EP, so that all EP request records are accessible if needed.
5. Any requests made through the AGCY0027 NAMS workflow for EP on that particular system must be addressed (not ignored or automatically rejected). It is up to the Center or

system owner how this is accomplished. This requirement is to ensure that users will not be penalized or ignored for using the Agency default EP NAMS workflow.

4.2 Do I need to create an EP NAMS workflow for my system?

No, this is optional (see section 4.1).

NASA OCIO has created a default EP NAMS workflow, which meets the policy requirements. This default EP NAMS workflow is called “AGCY0027 ElevPriv_Agency.”

It is up to the information system owner and Center CIOs to determine which NAMS workflow will be used to manage elevated privileges for their systems, from the following options:

1. If applicable, must use the AD Resource Management Account workflow.
2. Use the default EP NAMS workflow.
3. Create an EP NAMS workflow specific for their system(s).

If the AD Resource Management Account workflow or the default EP NAMS workflow is not used, it is the ISO’s or Center CIO’s responsibility to manage any administrative information in their chosen NAMS workflow (e.g. list of approvers, provisioners, etc.).

4.3 How do I create an EP NAMS workflow for my system?

See the Center Account Authorization Official (AAO) for help with creating a new EP NAMS workflow for your system. For a list of Center AAO’s, see:

http://insidenasa.nasa.gov/ocio/infrastructure/aao_POCs.html

Any new EP NAMS workflows must meet the requirements in NITR 2810-14A and section 4.1 of this handbook.

4.4 How do I use the default EP NAMS workflow as a requester?

As a requester, you will need several pieces of information to request elevated privileges through NAMS, which can be found as follows:

- The **SSP** that covers the device on which you need EP
 - Check with the ISO, ISSO, OCSO or Center ITSM
 - If you are the ISO, then it is the SSP number assigned to the SSP submitted when the system was C&A’d
- The name of the **device** on which you need EP
 - This is also known as the computer name, hostname, or machine name. On Windows computers, this can be found in the Control Panel\System application under the Computer Name tab.
- The name of your **sponsor**

- The sponsor is the requester's direct manager or supervisor who can confirm that the request is legitimate and that the requester does need these privileges to perform his or her tasks and duties.

Figure 4.4 provides step-by-step instructions for requesting EP using the default NAMS workflow.

To request EP on multiple devices, enter MULTIPLE in the Computer field in step 1 under Request Details. Then list or describe all the devices for which you need EP in the Notes field.

To request EP on multiple information systems (assuming that all of systems are using the default NAMS EP workflow), select all applicable ITSSPs in the ITSSP field in step 1 under Request Details. Then list or describe all the devices for which you need EP in the Notes field.

Step-by-step instructions for requesting EP using the default NAMS workflow

1. Log into IdMAX (<http://idmax.nasa.gov>) and fill out a request
 - Click on link for Request or Modify Application Account in the Account Management – NAMS - 4.2 section
 - In the User tab, select the user (if other than yourself)
 - In the Requester tab, select the requester (if other than yourself)
 - In the Sponsor tab, select the user's supervisor
 - In the Applications tab, type **elevated** into the keyword field to search for the application
 - Click the 'Add to Request' button next to the 'AGCY0027 ElevPriv_Agency' application
 - Click the 'Continue' button at the bottom of the screen
 - Under Request Details
 - For Computer, enter the computer name
 - For ITSSP, select the system which includes the computer
 - For UserID, enter the user's login name on the desktop/laptop which should be granted elevated privileges
 - Select the appropriate training that the user has completed
 - Read the User Acknowledgement Statement and accept it by checking the checkbox
 - Mark the Urgency of the request
 - Provide the reason or Business Justification for requesting the elevated privileges. This must include an explanation of what necessary actions cannot be performed without elevated privileges.
 - Enter any special instructions or notes if applicable
 - Click the 'Submit' button at the bottom of the screen
 - On the Confirm Application Account Request screen, review the information and click 'Confirm'. If information is incorrect, click 'Start Over'
 - On the Application Account Request screen, record the request number, and click 'Submit'
 - NAMS sends email confirmation to the requester that the request is pending
2. NAMS sends request email to sponsor; sponsor logs into NAMS and approves
3. NAMS sends request email to approver
4. Approver logs into NAMS
 - If the approver denies the request; NAMS sends deny email to requester; done
 - Approver approves justification
 - If training not met, approver sends email to requester to take training; user takes training; requester replies to approver that training is completed AND/OR requester updates request in NAMS
 - Approver validates that training has been taken
5. NAMS sends an email to the requester that request is completed
6. Approver forwards the NAMS email (from step 3 above), with an indication of the approval, to the provisioner.
7. Provisioner makes the necessary account changes.

Figure 4.4

4.5 How do I use the default EP NAMS workflow as a system owner?

The default EP NAMS workflow has to be maintained to accurately reflect the list of SSPs covering all of NASA's IT devices and the list of approvers at each Center.

The Agency OCIO is responsible for keeping the list of SSPs up-to-date in the default EP NAMS workflow. This information will be based on the authoritative list of NASA SSPs and will be updated as needed via an SR to the NEACC.

Each Center CIO is responsible maintaining the list of approvers for their Centers. Any changes should be submitted via an SR to the NEACC.

To submit an SR to the NEACC:

1. Go to <https://arsweb.msfc.nasa.gov/ifmuser.asp>.

2. If you do not already have a Remedy account, you may do a "Guest Submit".

Or, you may log into the Remedy Service Request systems using your Remedy credentials.

3. On the "IEM Information" tab, fill in the Title, Description, SR Type, Type, and Application to match the example. Complete your name and contact information.

Note: In the "Application drop-down list," select Identity Credential Access Mgmt (ICAM) → Logical Access Management → NAMS → Tools.

Attach a document that includes your Center, Name of the SSP, and a list of Approvers and/or Provisioners. The Approvers/Provisioners lists MUST include the UUPIC, First Name, and Last Name.

Figure 4.5.3 below, shows a screen shot of an example SR.

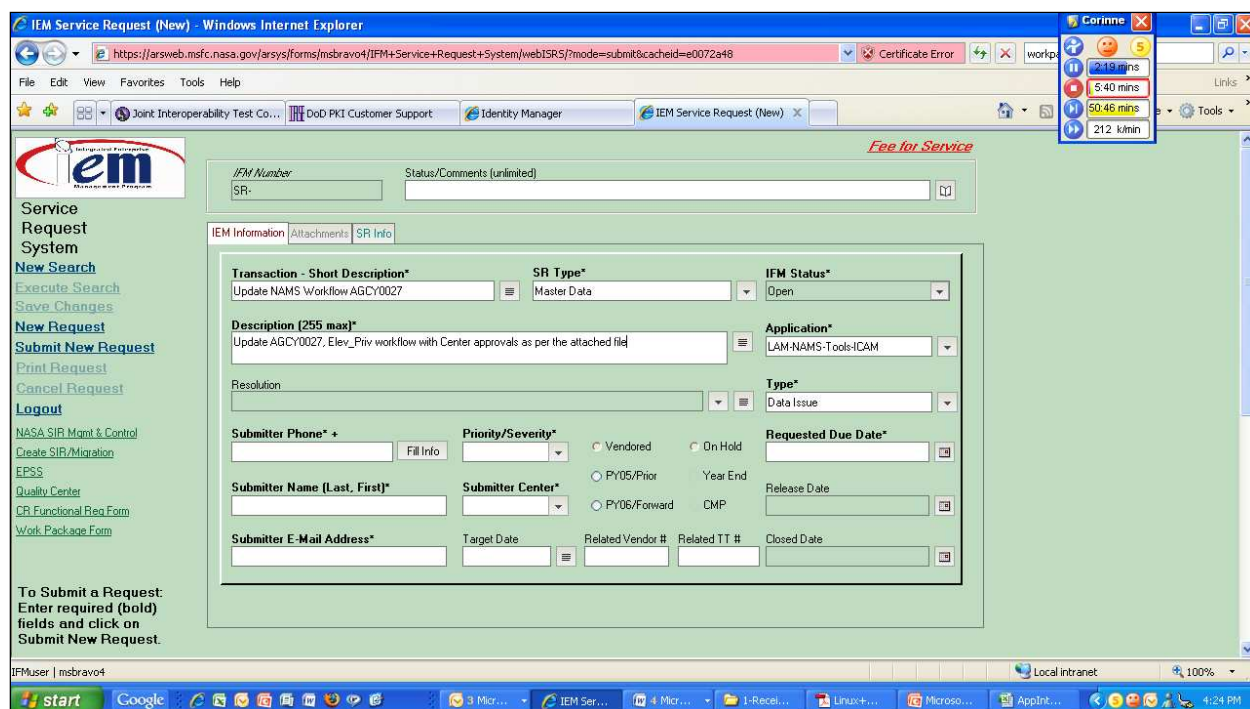


Figure 4.5.3

4. The workflow will be updated as part of the monthly release schedule for NAMS.

4.6 How do I use the default EP NAMS workflow as an approver?

For each request, the approver is the Center CIO, or their designee(s), of the requester's home Center. When a request is submitted, NAMS routes the request to all the designated approvers via email. The approver then logs into NAMS, reviews the business justification, and approves or denies the request as appropriate.

The default EP NAMS workflow does not automatically route approved requests to the provisioner because maintaining the routing flows for NASA's almost 600 systems is not feasible. Therefore, it is up to the approver to send approved requests to the provisioner(s) appropriate for the system on which the EP were requested. This can be done by forwarding the NAMS notification email, which contains all the relevant information, to the provisioner.

4.8 Additional questions...

1. What happens when a system administrator transitions from one contract to another?

Any change in role or responsibility for someone with EP requires that an updated NAMS request or revocation of existing EP be done promptly.

However, there is currently no automatic effect in NAMS when someone transfers to a new contract. The system administrator retains their elevated privileges, assuming their userid

does not change. In the future, NAMS will have the capability to send update information to the Approver when a contract changes.

2. How is expiration of EP requests enforced and how are the relevant people notified?

Currently NAMS does not support notifications and enforcement of request expiration, although this is planned for the future. Several Centers and the ODIN contractor are working on mechanisms to track and enforce request expiration outside of NAMS.

5. Training

5.1 What training is needed for whom/what kind of request?

If the user is using SATERN to meet the qualification requirements in section 1.3 of NITR 2810-14A, the following tables show which SATERN courses are needed.

Users	SATERN Courses
All users	Elevated Privileges on NASA Information System (ITS-002-09)
Users granted EP for longer than 30 days	Elevated Privileges on NASA Information System (ITS-002-09) AND IT Security for System Administrators – Beginning Level (ITS-RB1-SA)
System administrators	Elevated Privileges on NASA Information System (ITS-002-09) AND IT Security for System Administrators – Beginning Level (ITS-RB1-SA) AND IT Security for System Administrators – Intermediate Level (ITS-RB2-SA) AND An appropriate operating system course for each operating system on which the person will have EP. See Table 5.1.2 for acceptable SATERN operating system courses.

Table 5.1.1 SATERN training for users requesting elevated privileges

Operating System	SATERN Courses
WindowsXP	Backup and Security Settings in Microsoft Windows XP (SS-113758_ENG)
Windows Vista	Windows Vista Security and Performance Improvements (SS-242964_ENG)
Mac OS	Mac OS X Security (ITS-001-09)
Unix	Solaris 9 Security (SS-76291_ENG)
Linux	Security in a Linux Environment (SS-259948_ENG)

Table 5.1.2 SATERN training on operating systems

If the user is using other training, certifications, or work experience to meet the qualification requirements, see section 5.3.

5.2 When should a user take the training?

All users should take the Elevated Privileges Awareness SATERN training before submitting their request. This course takes only 30 minutes or less and provides basic information that anyone who is interested in holding elevated privileges on any NASA IT device should know.

It is up to the Center CIO (or designee), as the NAMS approver, to determine when requesters should take any training necessary to demonstrate their qualifications for holding elevated privileges. Some of the training can be lengthy and requesters may not want to take it until they are confident that their request will be approved. On the other hand, completing any required training ahead of submitting a request may speed up approval of the request.

Center CIOs (or designees) should establish and communicate to their users the preferred sequence of meeting qualification requirements, submitting requests for elevated privileges, etc. Some Centers have already implemented the following process, which appears to work well:

- If the requester and sponsor are confident that the request will be approved, the requester completes the training before submitting a request.
- Otherwise, the requester contacts the approver to see if a particular request is reasonable and likely to be approved.
- If so, the requestor then takes any necessary training and submits the NAMS request for EP.
- Training must be completed and verified to the approver's satisfaction before a request is approved.

5.3 Who determines what training is acceptable and how?

If the user is using SATERN to meet the qualification requirements, see question 5.1.

Otherwise, the Center CIO (or designee), as the NAMS approver, determines what training is acceptable and meets the policy requirements. Qualification requirements must be met for each operating system on which the person will have EP. Some professional qualifications that could be used to meet the operating system requirements, if approved, include the MSCE and GIAC certifications.

5.4 Who verifies that qualification requirements have been met?

The Center CIO (or designee), as the NAMS approver, is responsible for verifying that qualification requirements have been met. The validation method and level of assurance is left to the discretion of the Center CIO (or designee) and should be sufficient to let the Center CIO be comfortable with their approval decision. The Center CIO should consult with the system owner on determining a validation method and take into account the sensitivity of the system and the level of elevated privileges being granted.

An automated way to link NAMS requests for EP with checks of the SATERN training records is currently not available. The Center CIO (or designee) may choose to check SATERN training records manually to verify users' claims that they have taken the appropriate SATERN training. To do so, administrative access to SATERN is required.

5.5 Why are qualification requirements based on the length of the request instead of the level of privileges requested?

The level of qualification and training required before a user can hold elevated privileges is based on the level of risk incurred by the user holding those privileges. Ideally, qualification/training requirements would be determined by the level of privileges being granted. However, the large number of possible privilege levels makes it infeasible, at this time, to use privilege level as the measure of required qualifications.

The length of the request is used as the best alternative measure. The longer a user holds and uses elevated privileges on a NASA computer, the more likely it is that something detrimental will happen. For example, if a user has elevated privileges for just a few days to install software, it is less likely that the user will inadvertently download malware while surfing the Web during that time. On the other hand, if a user routinely logs into their computer with elevated privileges over an extended period of time, the likelihood increases of downloading malware or of changing system settings and causing a problem.

If the user is performing the duties of a system administrator, it is expected that they will change system settings and perform other administrative functions. Such a user must have the proper training and/or experience to perform these functions and to understand the consequences and risks of their actions on the computer.

6. Waivers

6.1 What kinds of waivers are possible and who can approve them?

Theoretically, any of the requirements in NITR 2810-14A can be waived. However, except for waivers of training requirements, waivers are not likely to be approved.

Per NITR 2810-14A, waivers to the policy must follow the NASA IT Waiver Process (NITR 2800-1). Waiver authority has been delegated from the NASA CIO to the Center CIOs, per the memorandum in Appendix D, for any waivers related to the qualification requirements in section 1.3 of the NITR. In other words, Center CIOs may approve waivers related to the training or certifications needed for individuals to demonstrate that they are qualified to hold elevated privileges.

Any other waivers of the requirements in the policy must be approved by the NASA CIO. The following are examples of requirements for which waivers must have NASA CIO approval:

- The requirement to manage elevated user privileges on a particular information system, group of systems, device, or group of devices

- The requirement to use NAMS for managing elevated user privileges

Waiver requests of requirements related to management of elevated user privilege must be for specific IT devices, specific information systems, or specific individuals requesting elevated privileges. Waiver requests must also be for specific time periods, not to exceed one year.

6.2 How do I get a waiver?

Follow the NASA IT Waiver Process detailed in NITR 2800-1.

6.3 How should waivers be tracked?

It is up to the Center CIOs and NASA CIO how to track waivers but there should be a record, paper or electronic of every approved waiver.

6.7 Can waivers be renewed?

Waivers cannot be automatically renewed. Any waiver (or renewal) must be reviewed and approved in accordance with the NASA IT Waiver Process as detailed in NPR 2800-1.

7. Miscellaneous

7.1 How will EP be managed on an ODIN device?

Requests for elevated privileges on ODIN-managed devices will be made using the AD Resource Management Account workflow or the default EP workflow (see section 4.1). Depending on the requester's home Center, the request will be routed to the appropriate Center CIO or designee for approval. For approved requests, the approver will then forwarding the NAMS email, with an indication of the approval, to ODIN for provisioning.

Appendix A. Acronyms

CIO	Chief Information Officer
CSIRT	Computer Security Incident Response Team
DoS	Denial of Service
DDoS	Distributed Denial of Service
EDCIRC	Department of Education Computer Incident Response Capability
EDNet	Department of Education Network
FISMA	Federal Information Security Management Act
IDS	Intrusion Detection System
IT	Information Technology
MAC	Media Access Control
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG/CCU	Office of Inspector General/Computer Crimes Unit
OMB	Office of Management and Budget
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
POC	Point of Contact
US-CERT	United States Computer Emergency Readiness Team

Appendix B. Definitions

This section lists common incident response terms and definitions as they appear in Appendix D of the NIST Computer Security Incident Handling Guide.

Agent: A program used in distributed denial of service (DDOS) attacks that sends malicious traffic to hosts based on the instructions of a handler.

Baselining: Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.

Blended Attack: Malicious code that uses multiple methods to spread.

Boot Sector Virus: A virus that plants itself in a system's boot sector and infects the master boot record.

Computer Forensics: The practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Computer Security Incident: See "incident."

Computer Security Incident Response Team (CSIRT): A capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center, Computer Incident Response Capability).

Denial of Service (DoS): An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

Distributed Denial of Service (DDoS): A DoS technique that uses numerous hosts to perform the attack.

Egress Filtering: The process of blocking outgoing packets that use obviously false Internet Protocol (IP) addresses, such as source addresses from internal networks.

Event: Any observable occurrence in a network or system.

False Positive: An alert that incorrectly indicates that malicious activity is occurring.

File Infector Virus: A virus that attaches itself to a program file, such as a word processor, spreadsheet application, or game.

File Integrity Checker: Software that generates, stores, and compares message digests for files to detect changes to the files.

Forensics: See "computer forensics."

Handler: A type of program used in DDOS attacks to control agents distributed throughout a network. Also refers to an incident handler, which refers to a person who performs incident response work.

Honeypot: A host that is designed to collect data on suspicious activity and has no authorized users other than its administrators.

Inappropriate Usage: A violation of acceptable computing use policies.

Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Incident Handling: The mitigation of violations of security policies and recommended practices.

Incident Response: See “incident handling.”

Indication: A sign that an incident may have occurred or may be currently occurring.

Ingress Filtering: The process of blocking incoming packets that use obviously false IP addresses, such as reserved source addresses.

Intrusion Detection System (IDS): Software that looks for suspicious activity and alerts administrators.

Macro Virus: A virus that attaches itself to documents and uses the macro programming capabilities of the document’s application to execute and propagate.

Malicious Code: A virus, worm, Trojan horse, or other code-based entity that infects a host.

Message Digest: A cryptographic checksum, typically generated for a file that can be used to detect changes to the file; Secure Hash Algorithm-1 (SHA-1) is an example of a message digest algorithm.

Mobile Code: Software that is transmitted from a remote system to a local system, then executed on the local system without the user’s explicit instruction; examples of mobile code software are Java, JavaScript, VBScript, and ActiveX.

Multiple Component Incident: A single incident that encompasses two or more incidents.

Packet Sniffer: Software that observes and records network traffic.

Patch Management: The process of acquiring, testing, and distributing patches to the appropriate administrators and users throughout the organization.

Port Scanning: Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).

Precursor: A sign that an attacker may be preparing to cause an incident.

Profiling: Measuring the characteristics of expected activity so that changes to it can be more easily identified.

Risk: The probability that one or more adverse events will occur.

Rootkit: A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker’s activities on the host and permit the attacker to maintain root-level access to the host through covert means.

Scanning: Sending packets or requests to another system to gain information to be used in a subsequent attack.

Signature: A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

Social Engineering: An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Threat: The potential source of an adverse event.

Trojan Horse: A non self-replicating program that seems to have a useful purpose, but in reality has a different, malicious purpose.

Unauthorized Access: A person gains logical or physical access without permission to a network, system, application, data, or other resource.

Victim: A machine that is attacked.

Virus: A self-replicating program that runs and spreads by modifying other programs or files.

Virus Hoax: An urgent warning message about a nonexistent virus.

Vulnerability: A weakness in a system, application, or network that is subject to exploitation or misuse.

Worm: A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Source: NIST Special Publication 800-61: *Computer Security Incident Handling Guide*,
<http://www.csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf>

Appendix C. References

Computer Security Act	Computer Security Act of 1987, P.L. 100-235 , as amended by P.L. 104-106
IA Security Policy	Department's Handbook for Information Assurance Security Policy (http://wdcrobiis08/doc_img/acs_hb_ocio_1.doc)
Departmental Directive	The Privacy Act of 1974 (The Collection, Use, and Protection of Personally Identifiable Information)
Privacy Act	Privacy Act of 1974, 5 U.S.C. § 552a
FISMA	Title III of the E-Government Act of 2002, the Federal Information Security Management Act (FISMA), P.L. 107-347
NIST SP 800-61	NIST Special Publication 800-61: Computer Security Incident Handling Guide. (http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf)
OMB A-130	Office of Management and Budget (OMB) Management of Federal Information Resources Circular A-130, Appendix III, November 28, 2000 (http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html)
OMB M-06-19	Office of Management and Budget (OMB) M-06-19: Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments (http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-19.pdf)

Appendix D: Memorandum Delegating Waiver Authority and Responsibility for Selected Requirements for Managing Elevated User Privileges on NASA IT Devices.

National Aeronautics and
Space Administration
Headquarters
Washington, DC 20546-0001



SEP 24 2009

Reply to Attn of:

Office of the Chief Information Officer

TO: Distribution

FROM: Chief Information Officer (Acting)

SUBJECT: Delegation of Waiver Authority and Responsibility for Selected
Requirements for Managing Elevated User Privileges on NASA IT
Devices

Requirements for managing elevated user privileges on NASA IT devices are stated in NITR 2810-14A, *Managing Elevated User Privileges on NASA IT Devices*.

The NASA IT Waiver Process requires:

1. That waivers to IT policies, procedures, standards or requirements standards, shall be granted by the NASA CIO; and
2. That the NASA CIO may delegate authority and responsibility to Center CIOs for a specific type of IT waiver or for a specific program or issue.

As permitted under the NASA IT Waiver Process, authority and responsibility for waivers of the following requirements are hereby delegated to the Center CIOs:

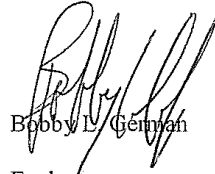
- Qualification requirements in section 1.3 of NITR 2810-14A.

Waiver authority and responsibility for all other requirements in NITR 2810-14A is retained by the NASA CIO. The following are examples of requirements for which waivers must have NASA CIO approval:

- The requirement to manage elevated user privileges on a particular information system, group of systems, device, or group of devices;
- The requirement to use NAMS for managing elevated user privileges; and
- The requirement to use a single NAMS workflow for all devices covered under a System Security Plan.

Requests for waivers of any requirements related to management of elevated user privilege must be for specific IT devices, specific information systems, or specific individuals requesting elevated privileges. Waiver requests must also be for specific time periods, not to exceed one year. All waiver requests must follow the NASA IT Waiver Process as identified in NITR 2800-1 (enclosed).

If you have any questions regarding this memorandum, please contact Marion Meissner at marion.meissner@nasa.gov or (202) 358-0585.

A handwritten signature in black ink, appearing to read "Bobby L. German". The signature is stylized with a large, looped "B" and a long, sweeping underline.

Enclosure

DISTRIBUTION:

Center CIOs:

ARC/Christopher Kemp
DFRC/Robert Binkley
GRC/Dr. Sasi Pillay
GSFC/Linda Cureton
HQ/Kelly Carter (Acting)
JPL/Jim Rinaldi
JSC/Larry Sweet
KSC/Mike Bolger
LaRC/Cathy Mangum
MSFC/Jonathan Pettus
NSSC/James Cluff (Acting)
SSC/Gay Irby

cc:

Center IT Security Managers:

ARC/Ernest Lopez
DFRC/Anthony Thomas
GRC/Don Cannatti
GSFC/Joshua Krage
HQ/Greg Kerr
JPL/Jay Brar
JSC/Ted Dyson
KSC/Henry Yu
LaRC/Kendall Freeman
MSFC/Walter Franklin
SSC/Christine Morreale
NSSC/James Cluff